



Text Part Number: 78-6608-03

Release Notes for the Catalyst 2900 Series XL and Catalyst 3500 Series XL Cisco IOS Release 12.0(5)XP

November 5, 1999

Cisco IOS Software Release 12.0(5)XP runs on Catalyst 3500 series XL switches and Catalyst 2900 series XL 8-MB switches. Catalyst 2900 series XL 4-MB switches are not supported in this release.

These release notes include important information about this release and any limitations, restrictions, and caveats that apply to it. See the “Related Documentation” section on page 21 for the complete list of Catalyst 2900 and 3500 XL switch documentation.

This IOS release is part of a special release of Cisco IOS software that is not released on the same 8-week maintenance cycle that is used for other platforms. As maintenance releases and future IOS releases become available, they will be posted to CCO in the Cisco IOS software area.

These release notes apply to the Cisco IOS Release 12.0(5)XP Enterprise Edition Software (-EN suffix) and the standard edition software (-A suffix). Those sections that make no reference to the Enterprise Edition Software apply to both editions.

Contents

This document has the following sections:

- “Important Notes” section on page 2
- “Hardware and Supporting Software” section on page 3
- “Changes Since IOS Release 11.2(8.x)SA6” section on page 4
- “Minimum IOS Release for Major Features” section on page 6
- “Limitations and Restrictions” section on page 7
- “Upgrading to a New Software Release” section on page 9
- “Current Caveats” section on page 18
- “Related Documentation” section on page 21
- “Cisco Connection Online” section on page 21
- “Documentation CD-ROM” section on page 22

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Copyright © 1999
Cisco Systems, Inc.
All rights reserved.

Important Notes

This section describes important information related to this IOS release.

Documentation Notes

Some of the hardware guides have not been updated for this release. References in these documents to IOS Release 11.2(8)SA6 are also valid for IOS Release 12.0(5)XP.

The titles of the *Quick Start: Catalyst 2900 Series XL Cabling and Setup* and *Quick Start: Catalyst 3500 Series XL Cabling and Setup* have been changed to *Quick Start Guide: Catalyst 2900 Series XL Switches* and *Quick Start Guide: Catalyst 3500 Series XL Switches*, respectively. References in other documents to the original document titles now apply to the documents with the new titles.

Browser Support

This release supports the platforms and network browsers described in Table 1.

Table 1 **Browser Support**

Operating System	Minimum Operating System Requirements	Netscape Communicator	Microsoft Internet Explorer
Windows 95	Service Pack 1	4.5, 4.51, or 4.61	4.01a or 5.0
Windows 98	Second Edition	4.5, 4.51, or 4.61	4.01a or 5.0
Windows NT 4.0	Service Pack 3	4.5, 4.51, or 4.61	4.01a or 5.0
Solaris 2.5.1 or higher	SUN-recommended patch cluster for the OS and Motif library patch 103461-24	4.5, 4.51, or 4.61	Not supported

Note Netscape Communicator version 4.60 is *not* supported.

The Quick Start guides include instructions for configuring Netscape Communicator and Microsoft Internet Explorer 4.01a. For instructions for configuring Microsoft Internet Explorer 5.0, refer to the *Cisco IOS Desktop Switching Software Configuration Guide*.

To use Cluster Management or Switch Network View applications, you need to complete the browser configuration as described in the *Cisco IOS Desktop Switching Software Configuration Guide*.

Hardware and Supporting Software

Table 2 lists the Catalyst 3500 XL switches supported by this IOS release, and Table 3 lists the 8-MB Catalyst 2900 XL switches supported by this IOS release. Table 4 lists the Catalyst 2900 and 3500 series XL modules and GBICs and their required IOS releases.

Note Catalyst 2900 Series XL 4-MB switches run original edition software and are not supported in this release. These switches cannot be updated to IOS Release 12.0(5)XP.

Table 2 Catalyst 3500 Series XL Switches

Model	Description	Number of VLANs	Standard Edition?	Enterprise Edition?	Command Capable?
WS-C3512-XL-EN WS-C3512-XL-A	12 autosensing 10/100 ports and 2 Gigabit Ethernet ports	250	Yes	Yes	Yes
WS-C3524-XL-EN WS-C3524-XL-A	24 autosensing 10/100 ports and 2 Gigabit Ethernet ports	250	Yes	Yes	Yes
WS-C3508G-XL-A WS-C3508G-XL-EN	8 Gigabit Ethernet ports	250	Yes	Yes	Yes
WS-C3548-XL-A WS-C3548-XL-EN	48 autosensing 10/100 ports and 2 Gigabit Ethernet ports	250	Yes	Yes	Yes

Table 3 8-MB Catalyst 2900 Series XL Switches

Model	Description	Number of VLANs	Standard Edition?	Enterprise Edition?	Command Capable?
WS-C2912MF-XL	12 100BaseFX ports and 2 high-speed expansion slots	250	No	Yes	With upgrade
WS-C2912-XL-A WS-C2912-XL-EN	12 autosensing 10/100 ports	64	Yes	Yes	With upgrade
WS-C2924M-XL-A WS-C2924M-XL-EN	24 autosensing 10/100 ports and 2 high-speed expansion slots	250	Yes	Yes	With upgrade
WS-C2924-XL-A WS-C2924-XL-EN	24 autosensing 10/100 ports	64	Yes	Yes	With upgrade
WS-C2924C-XL-A WS-C2924C-XL-EN	22 autosensing 10/100 ports and 2 100BaseFX ports	64	Yes	Yes	With upgrade

Table 4 Catalyst 2900 and 3500 Series XL Modules and GBICs

Model	Description	Minimum Release Required	VLAN Trunking Ports?
WS-X3500-XL	1 GigaStack GBIC	IOS Release 11.2(8)SA6	Yes, with a point-to-point connection (-EN only) ¹
WS-X2972-XL	1 ATM 155 SM-LR fiber port	IOS Release 11.2(8)SA5	Yes (-EN only)
WS-X2971-XL	1 ATM 155 SM-MR fiber port	IOS Release 11.2(8)SA5	Yes (-EN only)
WS-X2961-XL	1 ATM 155 MM fiber port	IOS Release 11.2(8)SA5	Yes (-EN only)
WS-X2951-XL	1 ATM 155 UTP port	IOS Release 11.2(8)SA5	Yes (-EN only)
WS-X2931-XL	1 1000BaseX port	IOS Release 11.2(8)SA5	Yes (-EN only)
WS-X2924-XL-V	4 100BaseFX ports	IOS Release 11.2(8)SA4	Yes, with minimum release of 11.2(8)SA5-EN
WS-X2922-XL-V	2 100BaseFX ports	IOS Release 11.2(8)SA4	Yes, with minimum release of 11.2(8)SA5-EN
WS-X2914-XL-V	4 autosensing 10/100 UTP ports	IOS Release 11.2(8)SA4	Yes, with minimum release of 11.2(8)SA5-EN
WS-X2922-XL	2 100BaseFX ports	IOS Release 11.2(8)SA	No
WS-X2914-XL	4 autosensing 10/100 UTP ports	IOS Release 11.2(8)SA	No

¹ GigaStack GBICs can operate in full-duplex point-to-point mode or in half-duplex stacking mode.

Changes Since IOS Release 11.2(8.x)SA6

This section describes new features and other changes that have been implemented in this IOS release. In addition to the described features, the release includes performance enhancements to the directory system cache, optimization of CPU usage, and the addition of the cluster MIB.

New Features

The following new features have been added in IOS Release 12.0(5)XP:

- Extended Cluster Member Functionality

With IOS Release 12.0(5)XP, Catalyst 1900 and Catalyst 2820 Ethernet switches are now supported as member switches of clusters. These switches must be running firmware version 9.00 (standard or Enterprise Edition) and are not capable of being command switches.

- RMON Support

In this release, you can configure remote monitoring (RMON) by using the command-line interface (CLI) or Simple Network Management Protocol (SNMP). You cannot configure RMON by using Cisco Visual Switch Manager (CVSM). As in previous releases, the switch continues to support four RMON 1 groups: alarms, events, history, and statistics. In previous releases, the RMON statistics were enabled for all ports; in this release, they are disabled on all interfaces by default. You must enable RMON statistics by using the CLI or SNMP.

You configure RMON alarms and events by using the global **config rmon alarm** and **config rmon event** commands. You can collect group history or group Ethernet statistics by using the configure interface mode **rmon collection history** or **rmon collection stats** commands.

For more information, see the complete IOS Release 12.0 documentation set. It is available through CCO by selecting **Service and Support>Technical Documents>Documentation Home Page>Cisco IOS Software Configuration>Cisco IOS Release 12.0**.

- Management VLAN Configuration

By default, the switch IP address belongs to VLAN 1, the default management VLAN interface. However, you can now configure any VLAN to be the management VLAN. Workstations connected to ports assigned to the management VLAN can establish IP connections to the switch and access to the CVSM and SNMP. For a static-access or multi-VLAN port to access one of these management interfaces, it must also belong to the management VLAN.

You first create the switch virtual interface using CVSM or the CLI **config interface** command on static-access, dynamic-access, multi-VLAN, and trunk ports (Enterprise Edition Software only), then enable the interface as the management VLAN; you cannot use SNMP to create or remove the management VLAN. Only one management VLAN can be active at a time and it is used only for IP-related protocols. If it is not VLAN 1, the management VLAN can be deleted.

Note Changing the management VLAN for a switch that is a member of a cluster disconnects the switch from the cluster. Refer to the *Cisco IOS Desktop Switching Software Configuration Guide* for more information.

- IEEE 802.1p Quality of Service

With Enterprise Edition Software, the Catalyst 2900 and 3500 XL switches provide Quality of Service (QoS) based on IEEE 802.1p class of service (CoS) values. QoS classifies frames by assigning priority-indexed CoS values to them and then gives delivery preference to higher-priority traffic. CoS values range from 0 for the lowest priority to 7 for the highest priority and are carried in the headers of Inter-Switch Link (ISL) and IEEE 802.1Q frames. Other frame types cannot carry CoS values.

When an untagged frames is received on a port, it is assigned the value of the ingress port default priority. A tagged frame uses its assigned CoS value when passing through the ingress port.

Note The WS-X2914-XL and WS-X2922-XL modules do not support this feature.

Note Before setting up QoS based IEEE 802.1p CoS on a Catalyst 2900 or 3500 XL switch interoperating with the Catalyst 6000 family of switches, you should refer to the Catalyst 6000 documentation. The Catalyst 6000 switches and the Catalyst 2900 and 3500 XL switches behave differently regarding the tag handling default, the ratio of high priority to low priority frames, and the buffer queue size. You should understand these differences to ensure compatibility.

Changes and Notes on Configuring the Switch

- You need privilege level 15 (the default privilege level) to access CVSM, Switch Network View, and the Cluster Management software. You must also use privilege level 15 if you configure TACACS+ (Enterprise Edition Software only) by using the CLI so that all your HTTP connections are authenticated through the TACACS+ server.

- When assigning IP information to a Catalyst 2900 or Catalyst 3500 XL switch, you are prompted to decide if you want to enable the switch as a cluster command switch. If yes (Y), you must then assign a name to the cluster.
- CVSM does not check parameter values that are outside the value range. If you enter an invalid parameter value, CVSM redisplay the page with the original value. Parameter value ranges are provided in the CVSM online help and in the *Cisco IOS Desktop Switching Command Reference* (online only).
- When configuring VLAN Trunk Protocol (VTP) for the first time in your network (Enterprise Edition software only), you must always assign a domain name. It is not necessary to assign a password, but if you assign a password to one switch, you must configure the same password on all other switches in the domain.

If you are adding a new switch to an existing network that has VTP capability, the new switch can learn the domain name from VTP advertisements sent by another switch on the network, but only after any applicable VTP password has been configured on the switch.

Hardware Notes

- The Catalyst 3548 XL switch ships with a new cable guide that secures up to 48 cables and mounts on the left side of the switch.
- If you plan to install the Catalyst 3548 XL switch in a rack, you must first remove screws in the switch chassis so that the mounting brackets can be attached to the chassis.
- In addition to the GBICs listed in the *Catalyst 3500 Series XL Installation Guide*, the Catalyst 3500 series XL switches also support the 1000BaseZX GBIC. You can use up to two 1000BaseZX GBICs with the Catalyst 3512, 3524 and 3548 XL switches; up to four ZX GBICs with the Catalyst 3508 XL switch. Catalyst 2900 series XL switches do not support 1000BaseZX GBICs.

Instructions and specifications in the *Cisco Gigabit Interface Converter Installation Note* apply to GBICs installed in Catalyst 3500 series XL switches as well as to those products referenced in the note.

Minimum IOS Release for Major Features

Table 5 lists the minimum IOS release required to support the major features of the Catalyst 2900 series and 3500 series XL switches.

Table 5 Catalyst 2900 and 3500 Series XL Features and the Minimum IOS Release Required

Feature	Minimum Release Required
Catalyst 3500 series XL switches (except 3548 XL)	IOS Release 11.2(8)SA6
Catalyst 3548 XL switch	IOS Release 12.0(5)XP
Cluster Management	IOS Release 11.2(8)SA6
Terminal Access Control Access Server+ (TACACS+)	IOS Release 11.2(8)SA6 (Enterprise Edition Software)
Network Time Protocol (NTP)	IOS Release 11.2(8)SA6
Spanning-Tree Protocol (STP) UplinkFast	IOS Release 11.2(8)SA6 (Enterprise Edition Software)
250 VLANs (some models; see the “Hardware and Supporting Software” section on page 3)	IOS Release 11.2(8)SA6

Table 5 Catalyst 2900 and 3500 Series XL Features and the Minimum IOS Release Required (continued)

Feature	Minimum Release Required
Catalyst 2900 series XL 1000BaseX modules	IOS Release 11.2(8)SA5
Catalyst 2900 series XL ATM modules	IOS Release 11.2(8)SA5
VLAN Management Policy Server (VMPS)	IOS Release 11.2(8)SA4 (Enterprise Edition Software)
8192 MAC addresses on modular switches	IOS Release 11.2(8)SA4
Inter-Switch Link (ISL) trunking	IOS Release 11.2(8)SA4 (Enterprise Edition Software)
IEEE 802.1Q trunking	IOS Release 11.2(8)SA5 (Enterprise Edition Software)
Switch Network View stack management	IOS Release 11.2(8)SA3
Web-based switch management	IOS Release 11.2(8)SA
Fast EtherChannel port groups	IOS Release 11.2(8)SA
Catalyst 1900 and Catalyst 2820 switches as cluster members	IOS Release 12.0(5)XP
RMON configuration through the CLI and SNMP	IOS Release 12.0(5)XP
Configuration of the Management VLAN	IOS Release 12.0(5)XP
IEEE 802.1p Quality of Service support	IOS Release 12.0(5)XP (Enterprise Edition Software)

Limitations and Restrictions

This section should be reviewed before you begin working with the switches. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

Connecting to the 600W Cisco Redundant Power System

The Cisco RPS can provide a quasi-redundant power source for four external devices that use up to 150W DC each. You can use a one-to-one cable (one connector at each cable end) to connect four external devices to the four DC output power modules. The power source is quasi-redundant because there are two AC input power modules for the Cisco RPS and one DC output power module for each external device. The AC input to the Cisco RPS is fully redundant, but the DC output to the external devices is not.

The following restrictions apply to using the 600W Cisco Redundant Power System (RPS) with a Catalyst 2900 or 3500 XL switch:

- The switches *do not* support the fully-redundant configuration described in the *Cisco RPS Hardware Installation Guide*.
- We recommend that you do not use the redundant-with-reboot configuration with the switch connected to the RPS and to the AC power plug, due to the reboot and downtime—approximately 30 seconds. If you do use the redundant with reboot configuration, always power up the switch before you power up the RPS to ensure correct operation. When the RPS powers up first, the LEDs might not indicate the actual state.
- If you are using an RPS with a revision level lower than Z3 with a Catalyst 3508G or a Catalyst 3548 XL switch, the RPS output connector DC status LED and the switch RPS LED might display amber (normally indicating an RPS malfunction) even when the RPS is functioning properly. The LEDs display correctly for RPS revision level Z3 or later. The label on the bottom of the RPS shows the revision level.

TACACS+ and CVSM

TACACS+ does not manage access authentication for Cisco Visual Switch Manager (CVSM). The switch password is used.

Hot-Swapping Not Supported for ATM and Gigabit Ethernet Modules

A Catalyst 2900 XL switch must be turned off before you can insert one of the following modules:

- Catalyst 2900 series XL 1000BaseX modules
- Catalyst 2900 series XL ATM modules

Port Configuration Conflicts

Certain combinations of port features create configuration conflicts (see Table 6). For example, the network port floods all unknown unicast and multicast packets to a port; therefore, port security, which limits traffic on a port, cannot be enabled on the network port. If you try to enable incompatible features, CVSM issues a warning message and prevents you from making the change. Reload the page to refresh CVSM.

In Table 6, *No* means that the two referenced features are not compatible.

Table 6 Port Configuration Conflicts

	ATM Port¹	Port Group	Port Security	Monitor Port	Multi-VLAN Port	Network Port	Connect to Cluster?
ATM port	–	No	No	No	No	No	Yes
Port group	No	–	No	No	Yes	Yes ²	Yes
Port security	No	No	–	No	No	No	Yes
Monitor port	No ³	No	No	–	No	No	Yes
Multi-VLAN port	No	Yes	No	No	–	Yes	Yes
Network port	No	Yes (only source-based group)	No	No	Yes	–	No ⁴
Connect to cluster	Yes	Yes	Yes	Yes	Yes	No	–

1 Catalyst 2900 series XL switches only

2 A network port cannot connect cluster members to the command switch.

3 An ATM port cannot be a monitor port, but it can be monitored.

4 Cannot connect cluster members to the command switch.

IEEE 802.1Q Configuration Considerations

IEEE 802.1Q trunks impose some limitations on the trunking strategy for a network. The following restrictions apply to IEEE 802.1Q trunks:

- Make sure the native VLAN for an IEEE 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.

- Disabling STP on the native VLAN of an IEEE 802.1Q trunk without disabling STP on every VLAN in the network can potentially cause STP loops. We recommend that you either leave STP enabled on the native VLAN of an IEEE 802.1Q trunk or disable STP on every VLAN in the network. Make sure your network is loop-free before disabling STP.

Spanning-Tree Maximum Age Command

The range of seconds for the **span-tree max-age** command is now 6 to 200 seconds. If you used this command in a release prior to 11.2(8)SA6 to set a value greater than this new range and then upgrade your software to IOS Release 11.2(8.1)SA6 or later, the switch sets this value to the default: 20 seconds for IEEE STP, 15 seconds for DEC STP, and 10 seconds for IBM STP.

SPAN Limitations

When using the Switched Port Analyzer (SPAN) feature, the monitoring port receives copies of transmitted and received traffic for all monitored ports. If the monitoring port is 50 percent oversubscribed for a sustained period of time, it will probably become congested. One or more of the ports being monitored might also experience a slowdown.

Compatibility with the CiscoWorks2000 RME Suite

When using the Software Image Management (SWIM) application in the Resource Manager Essentials (RME) suite of the CiscoWorks2000 product family to perform automated system software and boot loader upgrades, you should note the following:

- Catalyst 2900 series XL switches require IOS Release 11.2(8)SA4 or later and RME version 2.1 or 2.2.
- Catalyst 3500 series XL switches require IOS Release 11.2(8.1)SA6 or later and RME version 2.2.

Upgrading to a New Software Release

This section describes the procedure for upgrading your switch software by using the IOS command-line interface (CLI).



Caution The 4-MB Catalyst 2900 series XL switches do not have sufficient memory to be upgraded to this release.

If you are running IOS Release 11.2(8)SA3 or later, we recommend that you upgrade the switch by using the web-based CVSM because it is a much shorter procedure. General instructions for upgrading through CVSM are in the *Cisco IOS Desktop Switching Software Configuration Guide*; detailed instructions are provided in the CVSM help files.

Note When using CVSM or Cluster Manager to upgrade software for a switch, the “Retain Current IOS Image File Name” checkbox provides the following options:

- If selected, the new image copied to Flash memory has the same name as the previous image.
 - If deselected (the default), the new image copied to Flash memory keeps its current image name.
- In either case, only the new image exists in Flash memory.
-

Note You cannot use the web-based interface to upgrade a switch running IOS Release 11.2(8)SA2 or previous releases. Use the CLI to perform the upgrade in such cases.

The CLI upgrade procedure consists of the following major steps:

- Step 1** Downloading the combined .tar file from CCO. This file contains the IOS image and the HTML files. The **tar** command extracts the IOS image and the HTML files from the combined .tar file during the TFTP copy to the switch.
- Step 2** If necessary, downloading the TFTP server application to copy the switch software from your PC to the switch.
- Step 3** Using the CLI or CVSM to upgrade your switch to the new software.

Which Files to Use

Review Table 7 and Table 8 before you download the software. Table 7 describes the file extensions and what they mean for the upgrade procedure. It is easier to upgrade the switch software by using a combined .tar file that contains the HTML files and the IOS image. The upgrade procedures in these release notes describe how to use a combined .tar file, and you must use a combined .tar file to upgrade a switch through the switch HTML interfaces.

Table 8 describes the various versions of the software that can be downloaded. Each IOS version can support command-switch or member-switch capabilities. The software files for this IOS release are listed by switch in Table 9 and Table 10.

Table 7 Possible Extensions for IOS Software Files

Extension	Description
.tar	A compacted file from which you can extract files by using the tar command. There are two types of .tar files: <ul style="list-style-type: none"> • A <i>combined .tar</i> file that contains both the IOS image file and the HTML files. You can upgrade the switch software with this file from the CLI or from the CVSM System page. • An <i>HTML .tar</i> file that has the letters <i>HTML</i> in its name and contains just the HTML files for an IOS release. From the CLI, you can upgrade the switch software with this HTML file and the IOS image file.
.bin	The IOS image file that you can copy to the switch through TFTP.

Table 8 Possible Versions of IOS Software Files

IOS Version	Description
Standard edition software	The set of features that is available on all switches.
Enterprise Edition Software	The advanced set of features that is in addition to the standard edition software.
Cluster Management Capabilities	
Command switch	Software that enables the switch to be a cluster command switch.
Member switch	Software that enables the switch to be a cluster member switch.

Table 9 Catalyst 3500 Series XL Cisco IOS Software Files

Filename	Description	CCO Location ¹
c3500XL-c3h2-mz-120.5-XP.bin	Standard edition IOS image file	Registered and public
c3500XL-c3h2-mz-120.5-XP.tar	Standard edition IOS image file and HTML files	Registered and public
c3500XL-html-plus.120.5-XP.tar	Standard and Enterprise Edition Software HTML files	Registered and public
c3500XL-c3h2s-mz-120.5-XP.bin	Enterprise Edition Software IOS image file	Registered and public
c3500XL-c3h2s-mz-120.5-XP.tar	Enterprise Edition Software IOS image file and HTML files	Registered and public

¹ Software files are available through both a registered site, for which you must register to have access, and a public site for which there are no restrictions.

Table 10 Catalyst 2900 Series XL Cisco IOS Software Files

Filename	Description	CCO Location ¹
c2900XL-h2-mz-120.5-XP.bin	Standard edition IOS image-only file (member switch)	Registered and public
c2900XL-h2-mz-120.5-XP.tar	Standard edition IOS image and HTML files (member switch)	Registered and public
c2900XL-html.120.5-XP.tar	Standard and Enterprise Edition Software HTML files (member switch)	Registered and public
c2900XL-c3h2-mz-120.5-XP.bin	Standard edition IOS image-only file (command switch)	Registered only
c2900XL-c3h2-mz-120.5-XP.tar	Standard edition IOS image and HTML files (command switch)	Registered only
c2900XL-html-plus.120.5-XP.tar	Standard and Enterprise Edition Software HTML files (command switch)	Registered only
c2900XL-h2s-mz-120.5-XP.bin	Enterprise Edition Software IOS image-only file (member switch)	Registered and public
c2900XL-h2s-mz-120.5-XP.tar	Enterprise Edition Software IOS image and HTML files (member switch)	Registered and public
c2900XL-c3h2s-mz-120.5-XP.bin	Enterprise Edition Software IOS image-only file (command switch)	Registered only
c2900XL-c3h2s-mz-120.5-XP.tar	Enterprise Edition Software IOS image and HTML files (command switch)	Registered only

¹ Software files are available through both a registered site, for which you must register to have access, and a public site for which there are no restrictions.

Downloading the New Software

Follow these steps to download a new version of IOS 12.0(5)XP software and, if necessary, the TFTP server application.

Step 1 Use Table 7 to Table 10 to identify the file(s) that you want to download.

Note We recommend that you download the combined .tar file that contains the image file and the HTML files. The procedures in these release notes are for upgrading a switch by using a combined .tar file, and the web-based CVSM interface is designed to upgrade a switch by using this combined file.

Step 2 Registered users can download files from the following locations:

- For Catalyst 2900 XL switches, enter the following URL in your browser Go To or Location field:
<http://www.cisco.com/cgi-bin/tablebuild.pl/cat2900XL>
- For Catalyst 3500 XL switches, enter the following URL in your browser Go To or Location field:
<http://www.cisco.com/cgi-bin/tablebuild.pl/cat3500XL>

Un-registered users can download files from the following locations:

- For Catalyst 2900 XL switches:
<http://www.cisco.com/cgi-bin/tablebuild.pl/cat2900XL>
- For Catalyst 3500 XL switches:
<http://www.cisco.com/cgi-bin/tablebuild.pl/cat3500XL>

- Step 3** Download the IOS file or files.
- Step 4** Download the TFTP server from this URL, if necessary. The readme.txt file describes how to download the TFTP server.

After you have downloaded the correct file to your PC or workstation, you can use the CLI to perform a TFTP transfer of the file or files to the switch.

Upgrading Catalyst 3500 Series XL Switches

This procedure is only for upgrading 3500 XL switches by copying the combined .tar file to the switch. You copy the files to the switch from a TFTP server and extract the files by entering the **tar** command.

Follow these steps to upgrade the switch software by using a TFTP transfer:

- Step 1** If your PC or workstation cannot act as a TFTP server, copy the file to a TFTP server to which you have access.
- Step 2** Access the CLI by starting a Telnet session or by connecting to the switch console port through the RS-232 connector.

To start a Telnet session on your PC or workstation, enter the following command:

```
server% telnet switch_ip_address
```

- Step 3** Enter privileged EXEC mode:

```
switch> enable  
switch#
```

- Step 4** Display the name of the running (default) image file. The following example shows the name in italic:

```
switch# show boot  
BOOT path-list:    flash:current_image  
Config file:      flash:config.text  
Enable Break:     1  
Manual Boot:      no  
HELPER path-list:  
NVRAM/Config file  
buffer size: 32768
```

- Step 5** If there is no file defined in the BOOT path-list, enter **dir flash:** to display the contents of Flash memory.

- Step 6** Using the name of the combined .tar file that you downloaded, rename the running image file to that name, and replace the .tar extension with .bin. The image filename is then the same as the downloaded filename but with a .bin extension. This step does not affect the operation of the switch.

```
switch# rename flash:current_image flash:new_image
Source filename [current_image]?
Destination filename [new_image]?
```

For example:

```
switch# rename c3500XL-c3h2s-mz-112.8.2-SA6.bin c3500XL-c3h2s-mz-120.5-XP.bin
```

- Step 7** Display the contents of Flash memory to verify the renaming of the file:

```
switch# dir flash:
Directory of flash:
-rwx   1557283      Aug 17 1999 23:47:28  c3500XL-c3h2s-mz-120.5-XP.bin
-rwx     82475      Aug 17 1999 03:10:38  c3500XL-diag-mz-120.5-XP
-drwx   14144      Aug 17 1999 00:04:14  html
-rwx     2047      Mar 01 1993 18:46:01  config.text
-rwx         43      Jan 01 1970 00:00:34  env_vars

3612672 bytes total (1224704 bytes free)
```

- Step 8** Enter global configuration mode:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

- Step 9** Disable access to the switch HTML pages:

```
switch(config)# no IP http server
```

- Step 10** If you entered the **boot** command with the name of the image file, enter this command to change it to the new name:

```
switch(config)# boot system flash:new_image
```

Note If you have not entered the **boot** command with the name of the image, you do not need to enter this command; the switch automatically finds the correct file to use when it resets.

- Step 11** Return to privileged EXEC mode:

```
switch(config)# end
```

- Step 12** Remove the CVSM HTML files:

```
switch# delete flash:html/*
```

Press **Enter** to confirm the deletion of each file. Do not press any other keys during this process.



Caution In the following step, the **tar** command copies the combined.tar file that contains both the image and the HTML files. You do *not* need to copy an HTML.tar file in this procedure.

- Step 13** Enter the following command to copy the new image and HTML files to the switch Flash memory:

```
switch# tar /x tftp://server_ip_address//path/filename.tar flash:
Loading /path/filename.tar from server_ip_address (via VLAN1):!
extracting info (110 bytes)
extracting c3500XL-c3h2s-mz-112.0.66-SA6.bin (1271095 bytes)!!!!!!!!!!!!!!!!!!!!!!
html/ (directory)
extracting html/Detective.html.gz (1139 bytes)!
extracting html/ieGraph.html.gz (553 bytes)
extracting html/DrawGraph.html.gz (787 bytes)
extracting html/GraphFrame.html.gz (802 bytes)!
...
```

Depending on the TFTP server being used, you might need to enter only one slash (/) after the *server_ip_address* in the **tar** command.

- Step 14** Enter global configuration mode:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

- Step 15** Re-enable access to the switch HTTP pages:

```
switch(config)# IP http server
```

- Step 16** Return to privileged EXEC mode:

```
switch(config)# end
```

- Step 17** Reload the new software with the following command:

```
switch# reload
System configuration has been modified. Save? [yes/no]:y
Proceed with reload? [confirm]
```

- Step 18** Press **Return** to confirm the reload.

Your Telnet session ends when the switch resets.

- Step 19** After the switch reboots, you can use Telnet to return to the switch and to enter the privileged EXEC mode **show version** command to verify the upgrade procedure. If you have a previously opened browser session to the upgraded switch, you should close the browser and launch it again because the HTML files are now different.

Upgrading 8-MB Catalyst 2900 Series XL Switches

This procedure is for upgrading Catalyst 2900 XL switches with 8 MB of DRAM. You upgrade a switch by extracting the IOS image file and the HTML files from a combined.tar file. You copy the files to the switch from a TFTP server and extract the files by entering the **tar** command.

Note If you want to copy the IOS image file or HTML files separately to the switch, follow the upgrade procedure in the release notes that came with your switch, or refer to the Catalyst 2900 series XL release notes for IOS Release 11.2(8)SA4 on CCO.

If you are unsure whether your switch has 4 MB or 8 MB of memory, you can verify memory capacity at Step 4.

Follow these steps to upgrade the switch software by using the **tar** command to start a TFTP transfer:

Step 1 If your PC or workstation cannot act as a TFTP server, copy the file to a TFTP server to which you have access.

Step 2 Access the CLI by starting a Telnet session or by connecting to the switch console port through the RS-232 connector.

To start a Telnet session on your PC or workstation, enter the following command:

```
server% telnet switch_ip_address
```

Step 3 Enter privileged EXEC mode:

```
switch> enable
switch#
```

Step 4 Confirm that you have an 8-MB switch:

```
switch# show version
Cisco Internetwork Operating System Software IOS (tm)
C2900XL Software (C2900XL-HS-M), Version 11.2(8.2)SA6, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1998 by cisco Systems, Inc.
Compiled Mon 23-Nov-98 20:59 by paulines
Image text-base: 0x00003000, data-base: 0x00202144
```

```
ROM: Bootstrap program is C2900XL boot loader
```

```
2900XL-EN-84.3 uptime is 1 day, 22 hours, 23 minutes
System restarted by power-on
Running default software
```

```
→ cisco WS-C2924-XL (PowerPC403GA) processor (revision 0x11)
with 8192K/1024K bytes of memory.
Processor board ID 0x0E, with hardware revision 0x01
Last reset from power-on
```

```
Processor is running Enterprise Edition Software
24 Ethernet/IEEE 802.3 interface(s)
```

```
32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:50:80:39:EC:40
Motherboard assembly number: 73-3382-04
Power supply part number: 34-0834-01
Motherboard serial number: FAA02499G7X
Model number: WS-C2924-XL-EN
System serial number: FAA0250U03P
Configuration register is 0xF
```

Step 5 Display the name of the running (default) image file. The following example shows the name in italic:

```
switch# show boot
BOOT path-list: flash:current_image
Config file: flash:config.text
Enable Break: 1
Manual Boot: no
HELPER path-list:
NVRAM/Config file
buffer size: 32768
```

- Step 6** If there is no file defined in the BOOT path-list, enter **dir flash:** to display the contents of Flash memory. The file named *c2900XL-h2-mz-112.8.2.11-SA6.bin* is your image file.

```
switch# dir flash:
Directory of flash:
 3 ---x   80971      Sept 14 1998 03:10:38 c2900XL-h2-mz-112.8.2.11-SA6.bin
 4 d--x   14144      Mar 26 1993 23:17:47 html
 7 -rwx     84       Mar 26 1993 23:12:21 env_vars
 5 ---x    111      Mar 26 1993 23:12:23 info
258 ---x    111      Mar 26 1993 23:17:47 info.ver
230 -rwx   1470      Mar 26 1993 23:18:53 config.text

3612672 bytes total (1229312 bytes free)
```

- Step 7** Using the name of the combined .tar file that you downloaded, rename the running image file to that name, and replace the .tar extension with a .bin extension. The image file name is then the same as the downloaded file name but with a .bin extension. This step does not affect the operation of the switch.

```
switch# rename flash:current_image flash:new_image
Source filename [current_image]?
Destination filename [new_image]?
```

For example:

```
switch# rename flash:c2900XL-h2-mz-112.8.2-SA6.bin
flash:c2900XL-c3h2s-mz-120.5-XP.bin
Source filename [c2900XL-h2-mz-112.8.2-SA6.bin]?
Destination filename [c2900XL-c3h2s-mz-120.5-XP.bin]?
```

- Step 8** Enter global configuration mode:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

- Step 9** Disable access to the switch HTML pages:

```
switch(config)# no ip http server
```

- Step 10** If you entered the **boot** command with the name of the image file, enter this command to change it to the new name.

```
switch(config)# boot system flash:new_image
```

Note If you did not previously enter the **boot** command with the name of the image, you do not need to enter this command; the switch automatically finds the correct file to use when it resets.

- Step 11** Return to privileged EXEC mode:

```
switch(config)# end
```

- Step 12** Remove the HTML files:

```
switch# delete flash:html/*
```

Press **Enter** to confirm the deletion of each file. Do not press any other keys during this process.

- Step 13** If upgrading from IOS Release 11.2(8)SA5 or earlier, remove the files in the Snmp directory:

```
switch# delete flash:html/Snmp/*
```

Make sure the *S* in *Snmp* is uppercase.

Press **Enter** to confirm the deletion of each file. Do not press any other keys during this process.



- Caution** In the following step, the tar command copies the combined .tar file that contains both the image and the HTML files. You do not need to copy an HTML.tar file in this procedure.

- Step 14** Enter the following command to copy the new image and HTML files to the switch Flash memory:

```
switch# tar /x tftp://server_ip_address//path/filename.tar flash:
Loading /path/filename.tar from server_ip_address (via VLAN1):!
extracting info (111 bytes)
extracting c2900XL-c3h2s-mz-120.5.0-XP.bin (1557286 bytes)!!!!!!!!!!!!!!!!!!!!!!
html/ (directory)
extracting html/Detective.html.gz (1139 bytes)!
extracting html/ieGraph.html.gz (553 bytes)
extracting html/DrawGraph.html.gz (787 bytes)!
. . .
```

Depending on the TFTP server being used, you might need to enter only one slash (/) after the *server_ip_address* in the **tar** command.

- Step 15** Enter global configuration mode:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

- Step 16** Re-enable access to the switch HTTP pages:

```
switch(config)# IP http server
```

- Step 17** Return to privileged EXEC mode:

```
switch(config)# end
```

- Step 18** Reload the new software with the following command:

```
switch# reload
System configuration has been modified. Save? [yes/no]:y
Proceed with reload? [confirm]
```

- Step 19** Press **Return** to confirm the reload.

Your Telnet session ends when the switch resets.

- Step 20** After the switch reboots, you can use Telnet to return to the switch and enter the privileged EXEC mode **show version** command to verify the upgrade procedure. If you have a previously opened browser session to the upgraded switch, you should close the browser and launch it again because the HTML files are now different.

Current Caveats

This section describes possible unexpected activity by IOS Release 12.0(5)XP.

- When a Catalyst 2900 or 3500 series XL switch is configured as a cluster commander, it forwards frames in and out of the cluster. IP multicast packets with a broadcast MAC address, such as Enhanced Interior Gateway Routing Protocol (EIGRP) packets, that are received over a Gigabit interface can be duplicated or corrupted and forwarded back onto the network. The duplicate packets are sourced from the MAC address of the VLAN 1 interface. The destination MAC address is an entry in the switch ARP cache.

The workaround is to turn off receiving EIGRP multicast frames using the following commands:

```
switch (config) # access-list 100 deny eigrp any any
switch (config) # access-list 100 permit ip any any
switch (config) # int vlan1
switch (config-if) # ip access-group 100 in
```

(CSCdp15835)

- When you use CVSM to configure multiple port-related features, not all modifications are applied to all ports.

As a workaround, we recommend that you configure no more than 16 port-related features from one CVSM page. The number may be higher in some instances; the actual maximum number of features that can be configured at one time is dependent on the size of the http packet and the length of the configuration command. (CSCdp13730, CSCdm76306, CSCdm35873)

- If you try to access a switch by entering the IP address in the Cluster Builder or Cluster Manager browser page Location field, the Cisco Access page for the new switch opens. However, you cannot access Cluster Management from this page. The switch refreshes the Cisco Access page without launching Cluster Manager or Cluster Builder.

The workaround is to start a new browser session and enter the IP address of the new switch in the Location field of that browser session. (CSCdm91327)

- From the CVSM Cisco Discovery Protocol page, if you use Telnet or a browser to try to access a member switch that does not have an IP address configured for its management VLAN interface, the switch will access IP address 0.0.0.0. If the cluster member had an IP address that was cleared without the IP address being reassigned, the switch will try to Telnet or browse to the member's former IP address. However, you can use Telnet or a browser to access a member switch that has an IP address assigned to its management VLAN interface. Note that this behavior is different than in previous releases. In SA6, the switch Telnet or browser session would access the commander switch.

The workaround for Telnet is to first display the cluster-member number by entering the privileged EXEC command **show cluster member** from the commander switch CLI. Note the number of the member you want to access, and then use Telnet to return to the switch by entering the **recommand switch_number** command.

The workaround for the browser is to start Cluster Management from the switch home page and start Cluster Manager. Right-click or double-click the switch that you want to access, and select **Switch Manager**. (CSCdm34868)

- Links between members sometimes do not display in Cluster Builder or Cluster View.

The workaround is to display the Device Links Report from the Cluster Builder window. (CSCdm27668)

- On a Solaris platform, some dialog boxes in the Cluster Management application do not appear properly formatted, although they will function correctly.
Use Windows 95, Windows 98, or Windows NT 4.0 to avoid this problem. (CSCdm23953, CSCdm38744, and others)
- In Internet Explorer 5.0, the tab key does not work properly. It does not highlight the editable fields as it should.
Use the mouse to click on the field, or use Netscape 4.5, Netscape 4.51, Netscape 4.61, or Internet Explorer 4.01a. (CSCdm24761)
- When using Internet Explorer 5.0 and CVSM to change the configuration, changes are not updated by the browser but are applied to the switch.
The workaround is to click the browser **Refresh** button to display the new settings before making another change. If you do not Refresh before each change, the browser does not make the change. (CSCdm27546)
- A laptop computer that goes to sleep while it has an open serial port session to a Catalyst 3500 series XL switch can cause the switch to reset when the laptop wakes up.
The workaround is to disconnect the serial cable from the console port when it is not in use. (CSCdm37220)
- When you configure more than 64 VLANs and you do not save the running configuration, the switch can assign STP instances to the wrong VLANs the next time it reloads.
If you configure more than 64 VLANs on a Catalyst 2900 or 3500 XL switch, enter a privileged EXEC mode **save running-config** command after exiting VLAN configuration mode. (CSCdm33358)
- When a switch port configured as a multi-VLAN port is connected to a multi-VLAN port on another switch, continuous error messages display on the console terminal at a very fast rate.
The workaround is to not connect a multi-VLAN port to another multi-VLAN port. Multi-VLAN ports should be used for connecting the switch to end hosts and servers. (CSCdm75839)
- When using the SNMP management application to read an empty ATM LAN Emulation Client (LEC) MIB table, the switch might lose connectivity from the application. This problem is only seen if the ATM module does not have any LECs configured and “get-next” requests are sent to the ATM module polling multiple objects within one of the LEC tables. A loss of connectivity is not necessarily seen with all SNMP manager applications.
The workaround is either to not use an SNMP management station to poll the ATM module LEC tables when no LECs are configured, or to configure one or more LECs on the ATM module. (CSCdm75321)
- When a VLAN other than the default (VLAN 1) is set as the management VLAN, Switched Port Analyzer (SPAN) functions correctly on the command switch and on cluster member switches that have assigned IP addresses, but does not work on member switches that do not have IP addresses.
The workaround is to only use the default management VLAN or, if using another VLAN as the management VLAN, to assign IP addresses to those member switches where you want to use SPAN. (CSCdm62851)
- If you use the CLI **ip http port** command to try to change the default http port from port 80 to any other port, CVSM does not function properly.
The workaround is to not use this command and always use the default http port (port 80). (CSCdp07965)

- The **show spanning-tree interface** <interface> command correctly shows the count of received Bridge Protocol Data Units (BPDUs) incrementing on the blocking port, but the count of BPDUs sent from the forwarding port is always shown as zero.

The workaround is to use the **show interface** <interface> **account** command to view the correct count of BPDUs transmitted. (CSCdp03989)

- On the Catalyst 3548 XL switch, the bandwidth utilization LEDs do not correctly function as described in the *Catalyst 3500 Series XL Installation Guide*. (CSCdm92696)
- When using Cluster Builder or Cluster Manager to make changes to the cluster or to switches, if you then issue a **reload** command from the command or member switch CLI, you might not receive the “System configuration has been modified” message prompting you to save the changes. In that case, after the reload, the changes are not saved.

The workaround is to always save the configuration before issuing a **reload** command from the command or member switches. Changes made through the CLI and Switch Manager work as expected. (CSCdp06578)

- When using Cluster Builder on a UNIX Solaris platform, switches individually selected from the Suggested Candidate window are not added to the cluster after you enter the password and click OK. When you select all the suggested candidates or when you are in a Windows environment, the switches are successfully added to the cluster.

One workaround is to add candidates from the Cluster Builder layout window by right-clicking on the candidate and selecting **Add to Cluster...** from the pop-up menu. From the Suggested Candidates window, the workaround is to select the candidate by clicking the selected switch information in a column other than the first (Name) column. When you click on a switch row, the row is highlighted in every column except the one in which you clicked. If the Name row is not highlighted, the switch is not added to the cluster. If you click in the Device Type, MAC Address, or Upstream Switch column, the switch Name is highlighted, and the switch is added to the cluster. (CSCdm71746)

- IP access lists can interfere with creating clusters. If you filter VTY connections based on an IP access list, clustering can fail, and users cannot use the privileged EXEC mode **rcommand** to access the CLI for a member switch.

The workaround is to not use access lists if you want to cluster switches. The access class 199 that is created when a device is configured as the command switch is an exception. (CSCdm39364)

- Entering the interface configuration mode **no ip address** command to remove the IP address from a member switch disables the switch IP protocol stack.

The workaround is to enter the EXEC mode **clear ip address vlan 1** command instead. (CSCdm39373)

- Network Address Translation (NAT) commands are added to the configuration file of a command switch when a cluster is created.

No workaround is necessary, but the commands should not be removed. (CSCdm39380)

- When you issue a **show interface vlan 1** command, the number of collisions displayed might not be correct. (CSCdp16930)

- The Catalyst 1900 and Catalyst 2820 switches do not support the hidden-enable password. If one of these switches inherits a hidden-enable password from a cluster command switch, it stores the password as an unencrypted password. When your cluster contains Catalyst 1900 and Catalyst 2820 member switches, we recommend that you assign a secret enable password to the command switch and do not use a hidden-enable password. (CSCdp16523)

Related Documentation

The product documentation for the 3500 and 2900 XL switches and modules is as follows:

Catalyst 2900 Series XL Installation Guide

Quick Start Guide: Catalyst 2900 Series XL Switches

Catalyst 3500 Series XL Installation Guide

Quick Start Guide: Catalyst 3500 Series XL Switches

Cisco IOS Desktop Switching Software Configuration Guide for Cisco IOS Software Release 12.0(5)XP

Cisco IOS Desktop Switching Enterprise Edition Software Configuration Guide

Cisco IOS Desktop Command Reference (online only)

Catalyst 2900 Series XL Modules Installation Guide

Catalyst 2900 Series XL Gigabit Ethernet Module Installation Guide

Catalyst 2900 Series XL ATM Modules Installation and Configuration Guide

Release Notes for the Catalyst 2900 Series XL ATM Modules

Catalyst GigaStack Gigabit Interface Converter Installation Guide

Release Notes for Catalyst GigaStack Gigabit Interface Converter

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Access Registrar, AccessPath, Any to Any, AtmDirector, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, the Cisco Technologies logo, ConnectWay, Fast Step, FireRunner, GigaStack, IGX, Internet Quotient, Kernel Proxy, MGX, MultiPath Data, MultiPath Voice, Natural Network Viewer, NetSonar, Network Registrar, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, Secure Script, ServiceWay, SlideCast, SMARTnet, *The Cell*, TrafficDirector, TransPath, ViewRunner, Virtual Service Node, VisionWay, VlanDirector, WebViewer, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, GeoTel, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (9910R)

Copyright © 1999, Cisco Systems, Inc.
All rights reserved.